THE HONORABLE JOHN H. CHUN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JACINDA DORIAN, individually, and on behalf of all others similarly situated, Plaintiff, v. AMAZON WEB SERVICES, INC., Defendant.	No. 2:22-cv-00269-JHC AMAZON WEB SERVICES, INC.'S RULE 12(b)(6) MOTION TO DISMISS AND RULE 12(f) MOTION TO STRIKE CLASS ALLEGATIONS NOTE ON MOTION CALENDAR: June 10, 2022 ORAL ARGUMENT REQUESTED

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF CONTENTS

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF AUTHORITIES

Page(s)

CASES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

STATUTES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

RULES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

INTRODUCTION

This case is a brazen attempt to expand the Illinois Biometric Information Privacy Act ("BIPA") far beyond what its authors could have possibly intended. It should be dismissed in its entirety and with prejudice under Federal Rule of Civil Procedure ("Rule") 12(b)(6).

Plaintiff Jacinda Dorian is an Illinois resident. She claims that she took multiple remote tests (i.e., "take home" tests) while attending two colleges in Illinois. To protect the integrity of those tests, her colleges required her to use an online test proctoring service provided by ProctorU, Inc. ProctorU, in turn, required Plaintiff to submit an image of herself, and an image of a valid identification document, to ProctorU. According to Plaintiff, ProctorU then uploaded those images to its Amazon Web Services ("AWS") account and used AWS's Rekognition software to compare the images in order to verify Plaintiff's identity.

Plaintiff does not allege that she interacted with AWS in any way, or that AWS was even aware of her use of ProctorU's service. Nor does she allege that AWS, a Delaware corporation with its headquarters in Seattle, committed a single act in Illinois. Nevertheless, Plaintiff seeks to hold AWS liable under BIPA, an Illinois law that governs the possession and collection of biometric data. Curiously, Plaintiff has chosen not to sue her colleges, which "requir[ed]" her to use ProctorU's service, or ProctorU, which "required" her to submit images of herself and then analyzed those images to confirm her identity—suggesting strongly that this case is motivated by AWS's deep pockets rather than any actual harm to Plaintiff. Compl. ¶¶ 38, 39.[1]

[1] Notably, Plaintiff does not allege that ProctorU failed to meet BIPA's requirements when collecting and processing her images. In fact, discovery will show that ProctorU did comply with BIPA, which will provide an additional basis for dismissing Plaintiff's claims against AWS. *See Thakkar v. ProctorU, Inc.*, No. 21-CV-2051, 2021 WL 5507041, at *1 (C.D. Ill. Nov. 23, 2021) (explaining that, "[b]efore taking any online exam proctored by ProctorU, test-takers must affirmatively consent to ProctorU's Terms of Service" and Privacy Policy); *see also id.*, Dkt. 21-1 (Ex. 1) ¶ 3 (ProctorU's Terms of Service, which inform test-takers like Plaintiff that their use of ProctorU's service is governed by ProctorU's Terms of Service and ProctorU's Privacy Policy); *id.*, Dkt. 21-1 (Ex. 2) at 2 (ProctorU's Privacy Policy, which informs test-takers, among other things, that ProctorU's service "require[s] you to share your photo ID on camera," and that ProctorU "use[s] that ID in conjunction with biometric facial recognition software to authenticate your identity").

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

In any case, Plaintiff's novel attempt to sue AWS, which acted as nothing more than a "behind-the-scenes" cloud-services provider for ProctorU, fails for multiple reasons. *Id.* ¶ 5.

First, Plaintiff's attempt to sweep mere back-end service providers into BIPA's scope is inconsistent with any rational reading of the law. Plaintiff does not, and cannot, allege that AWS "possessed" or "collected" her data within the meaning of BIPA, and she therefore cannot allege that BIPA applies to AWS at all. Further, interpreting BIPA to apply to AWS in this case would produce absurd and unworkable results that this Court cannot condone.

Second, BIPA does not apply outside Illinois, so Plaintiff must allege that AWS's purported violations "occurred primarily and substantially in Illinois." *Avery v. State Farm Mut. Auto. Ins.*, 216 Ill. 2d 100, 187 (2005). But Plaintiff does not allege that AWS engaged in *any* conduct in Illinois. And applying BIPA to AWS's wholly out-of-state conduct, as Plaintiff seeks to do, would violate the U.S. Constitution's Dormant Commerce Clause.

Third, BIPA itself provides that the law's requirements may not be applied "in any manner" to "financial institutions" subject to the federal Gramm-Leach-Bliley Act, 740 ILCS 14/25(c), which includes Plaintiff's colleges. Forcing AWS to comply with BIPA's requirements in this context inevitably would force Plaintiff's colleges to comply with BIPA, too. The plain language of BIPA forbids that result and requires dismissal of Plaintiff's claims.

Fourth, Plaintiff is not "aggrieved" by AWS's purported failure to publish a biometric data retention policy under Section 15(a) of BIPA—an essential element of her claim. Plaintiff's Section 15(a) claim must be dismissed for that additional and independent reason.

Finally, even if Plaintiff could adequately allege BIPA claims against AWS (she cannot), her class allegations must be stricken under Rule 12(f) because they are patently overbroad.

Plaintiff may or may not have valid BIPA claims against her colleges or against ProctorU, the entities that required her to do the things of which she complains. But she certainly has no claims against AWS, which has no relationship to Plaintiff and merely acted as a back-end, out-of-state service provider for ProctorU. Plaintiff's claims should be dismissed.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

BACKGROUND

A. The Illinois Biometric Information Privacy Act ("BIPA")

Plaintiff's claims arise exclusively under BIPA, an Illinois state law. BIPA was enacted in 2008 in reaction to the growing use of biometric technology "in the business and security screening sectors," and to address the concerns of members of the public who were "weary of the use of biometrics when such information is tied to finances and other personal information." 740 ILCS 14/5(a), (d). Recognizing that "[t]he use of biometrics . . . appear[ed] to promise streamlined financial transactions and security screenings," the Illinois General Assembly sought to allay the public's concerns by regulating private companies' use of such data. *Id*.

BIPA specifically regulates "biometric identifiers" and "biometric information." A "biometric identifier" means a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. "Biometric information" means any information "based on" a biometric identifier. *Id*. For brevity, AWS refers to "biometric identifiers" and "biometric information" collectively as "biometric data."[2]

Equally important, BIPA does not prohibit the collection and use of biometric data entirely. Rather, it imposes requirements and obligations on private entities if they engage in certain activities with respect to biometric data. For example, under Section 15(a) of BIPA, companies "in possession" of biometric data must develop and comply with "a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying" biometric data within certain timeframes set out in the law. 740 ILCS 14/15(a). And under Section 15(b), companies that "collect . . . or otherwise obtain" biometric data must provide certain notices and obtain consent before doing so. 740 ILCS 14/15(b).

[2] By referring to "biometric data" throughout this motion, AWS does not in any way concede that it collected, possessed, stored, or otherwise obtained or used any data governed by BIPA. Further, AWS specifically reserves the right to argue, at the appropriate time, that even if it did collect, possess, store, or otherwise obtain or use any data regarding Plaintiff—a point AWS does not concede—no such data qualifies as "biometric identifiers" or "biometric information" within the meaning of BIPA.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

BIPA's penalties are harsh. "Any person aggrieved" by a violation of the law may sue for actual damages or, alternatively, liquidated damages of $1,000 per violation (for negligent violations) or $5,000 per violation (for "intentional[]" or reckless[]" violations). 740 ILCS at 14/20(1), (2). A prevailing party also may recover attorneys' fees and costs. *See* 740 ILCS 14/20(3). The potential for enormous recoveries has inspired a wave of more than 1,500 putative BIPA class actions in recent years. *See* Declaration of Ryan Spear ("Spear Decl.") ¶ 2; *see also id*., Ex. A (U.S. Chamber of Commerce Institute for Legal Reform, *A Bad Match: Illinois and the Biometric Information Privacy Act* at 4, 7 (Oct. 2021)) (noting the "exponential growth in BIPA litigation," which has disproportionately targeted "small companies" in Illinois).

B. Amazon Web Services ("AWS"), Rekognition, and ProctorU

AWS is "one of the largest providers of cloud computing services," offering its customers "over 200 cloud-based services from data centers globally." Compl. ¶¶ 1-2. As the Ninth Circuit has explained, the term "cloud computing" is "based on the industry usage of a cloud as a metaphor for the ethereal internet. . . . An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google." *United States v. Cotterman*, 709 F.3d 952, 965 n.12 (9th Cir. 2013) (internal quotation marks and citation omitted). In practical terms, AWS's cloud services allow AWS customers, like ProctorU, to remotely access, use, and control computer servers maintained by AWS to store and process the customers' own data, however the customers see fit. "Millions of customers—from startups to the largest enterprises—use AWS every day." Compl. ¶ 2.

One of the cloud-based services that AWS provides to its customers is a software product called "Rekognition." *Id*. ¶ 3. According to Plaintiff, Rekognition "uses machine vision and algorithmic classification techniques" to analyze electronic images, including images of faces. *Id*. Plaintiff alleges that AWS customers may upload electronic images to their cloud-storage accounts at AWS (known as "S3 buckets") and then run a Rekognition command called "index-faces" to extract biometric data from those images of faces. *Id*. ¶¶ 24-29. Plaintiff further alleges

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

that AWS customers may then use Rekognition's "face-matching" command to determine whether the same person appears in two or more images, and to generate a "similarity" score, i.e., "a confidence measurement to indicate how strongly Rekognition believes these faces match." *Id.* ¶ 31.

ProctorU is one of "[t]housands" of companies that incorporate Rekognition into their own products and services. *Id.* ¶¶ 4, 33. ProctorU allegedly "develops and licenses online test proctoring software for use by students and educational facilities." *Id.* ¶ 33. When a "student takes a test using ProctorU's proctoring software, ProctorU requires students to show their faces and their photo IDs on camera to help verify their identities." *Id.* ¶ 34. And "when [those students] upload their images to ProctorU," ProctorU "uses Rekognition" to compare the images and confirm test-takers' identities based on those images. *Id.* ¶ 35.

Importantly, Plaintiff (1) does not allege that AWS plays any role in this process beyond allowing ProctorU to access Rekognition and ProctorU's S3 buckets; (2) does not allege that ProctorU's S3 buckets are located in Illinois, or that AWS engaged in *any* conduct in Illinois; (3) does not allege that AWS controls the data in ProctorU's S3 buckets or is able to access it; and (4) does not allege that AWS interacts with or could interact with ProctorU's users. Indeed, Plaintiff does not even allege that AWS *knows* when ProctorU collects and stores students' data, let alone that AWS knows when ProctorU collects and stores data from students in Illinois.

C. Plaintiff's Claims Against AWS

Plaintiff's claims are based entirely on her use of ProctorU's service. Plaintiff alleges that she "took multiple tests" at two Illinois schools (the "Colleges") between 2017 and 2019. *Id.* ¶¶ 37, 38. The Colleges "requir[ed]" Plaintiff to use ProctorU's service to take her tests. *Id.* ¶ 38. ProctorU, in turn, "required" Plaintiff "to submit her image as well as an image of a valid identification document in order to be identified." *Id.* ¶ 39; *see also id.* ¶ 34 (ProctorU "requires" students to submit images to ProctorU). Plaintiff alleges that ProctorU then used the Rekognition service to confirm her identity based on the images she submitted to ProctorU. *See id.* ¶ 40.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Based on those allegations, Plaintiff asserts two claims against AWS. First, she alleges that AWS violated Section 15(a) of BIPA by "possess[ing]" her biometric data—that is, the data ProctorU collected and then uploaded to ProctorU's S3 bucket—without publishing "a publicly-available retention and deletion schedule." *Id.* ¶ 43. Second, Plaintiff alleges that AWS violated Section 15(b) of BIPA by "collect[ing]" that same data without providing the notice, and obtaining the consent, that Section 15(b) requires when companies collect biometric data. *See id.* ¶¶ 41-42. Plaintiff asserts both claims on behalf of herself and "[a]ll Illinois residents who had their biometric information or biometric identifiers collected, captured, received, possessed, or otherwise obtained by Amazon's Rekognition service and stored in AWS's servers." *Id.* ¶ 44.

For the reasons below, Plaintiff's claims should be dismissed, and Plaintiff's improper class allegations should be stricken.

MOTION TO DISMISS UNDER RULE 12(b)(6)

A. AWS Did Not "Possess" or "Collect" Plaintiff's Data

As a threshold matter, Plaintiff's BIPA claims fail because she cannot allege the most essential elements of those claims. Plaintiff cannot allege that AWS "possessed" her data for purposes of Section 15(a) because she cannot allege that AWS exercised any control or authority over that data. Similarly, Plaintiff cannot allege that AWS "collected" her data under Section 15(b) because Plaintiff's own allegations make clear that AWS never took any active steps to acquire or obtain her data; rather, it was ProctorU that collected Plaintiff's data. And as explained below, departing from those common-sense readings of BIPA's language would lead to a series of absurd and unworkable results. Plaintiff's claims should therefore be dismissed.[3]

[3] As the Court knows, dismissal under Rule 12(b)(6) "can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation marks and citation omitted). Dismissal should be with prejudice where, as here, the flaws in a complaint could not be cured by repleading. *See, e.g.*, *Williams v. Nat'l Football League*, No. C14-1089, 2014 WL 5514378, at *4 (W.D. Wash. Oct. 31, 2014), *aff'd*, 671 F. App'x 424 (9th Cir. 2016).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

1. Plaintiff alleges no facts showing that AWS "possessed" her data.

Section 15(a) applies only to private entities "in possession of" biometric data. 740 ILCS 14/15(a). But Plaintiff does not, and cannot, allege any facts showing that AWS possessed her data within the meaning of Section 15(a).

BIPA does not define "possession." Courts therefore "assume the legislature intended for it to have its popularly understood meaning." *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019) (citations omitted). The Illinois Supreme Court has explained that "possession, as ordinarily understood, occurs when a person *has or takes control* of the subject property or *holds the property at his or her disposal*." *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (internal quotation marks omitted) (emphasis added); *see also* Ill. Crim. Pattern Jury Instr. 4.16 ("actual possession" is "immediate and exclusive control over a thing" and "constructive possession" is "both the power and the intention to exercise control over a thing"). The Ninth Circuit interprets "possession" similarly. *See, e.g.*, *United States v. Kuchinski*, 469 F.3d 853, 861 (9th Cir. 2006) (possession in "electronic context[s]" requires a showing that the person "exercises dominion and control over" the relevant material); Ninth Cir. Crim. Model Jury Instr. 6.15 ("A person has possession of something if the person knows of its presence and has physical control of it, or knows of its presence and has the power and intention to control it.").

Here, Plaintiff does not allege that AWS controlled or held at its disposal the data that Proctor U allegedly uploaded to its S3 bucket. *See Ward*, 830 N.E.2d at 560. In fact, Plaintiff does not even allege that AWS "kn[ew] of [the] presence" of that data, Ninth Cir. Crim. Model Jury Instr. 6.15—an unsurprising omission, given that AWS has "[m]illions" of customers, Compl. ¶ 2, each of which may have up to 1,000 S3 buckets in their accounts, *see* Spear Decl., Ex. B at 1 ("Bucket restrictions and limitations" page from AWS's website).[4]

[4] Plaintiff's Complaint relies extensively on AWS's website. *See, e.g.*, Compl. ¶¶ 23-25. The Court may therefore consider other portions of AWS's website, and documents available on AWS's website, under the incorporation by reference doctrine. *See, e.g.*, *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005); *Loomis v. Slendertone Distrib., Inc.*, 420 F. Supp. 3d 1046, 1063 (S.D. Cal. 2019).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Plaintiff's failure to allege that AWS controlled ProctorU's data is fatal to her Section 15(a) claim. And no amount of repleading could cure that defect because AWS simply does not own or control that data. As the publicly available AWS Customer Agreement makes clear, AWS does not "access or use . . . Content [of AWS customers like ProctorU] except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." Spear Decl., Ex. C ¶ 3.2. The AWS Customer Agreement further provides that AWS customers must "ensure that [their] Content and [their] and End Users' use of [their] Content or the Service Offerings will not violate any of the [AWS] Policies or any applicable law." *Id.* ¶ 4.2. And it states, in no uncertain terms, that AWS customers "are solely responsible for the development, content, operation, maintenance, and use of [their] Content." *Id.* Thus, ProctorU "maintain[s] *full control*" of any "content that [it] upload[s] to" AWS's servers, and AWS does "not access or use [the] content for any purpose without [ProctorU's] agreement." Spear Decl., Ex. D at 1 (AWS Data Privacy FAQ) (emphasis added).

Plaintiff's own allegations are entirely consistent with those publicly available terms and disclosures. She herself alleges that only ProctorU exercised control over her alleged biometric data, and thus that only ProctorU "possessed" that data within the meaning of BIPA. *See Ward*, 830 N.E.2d at 560. According to Plaintiff, it was ProctorU that "required [her] to submit her image as well as an image of a valid identification document in order to be identified," Compl. ¶ 39; it was ProctorU that allegedly "perform[ed] facial recognition on" the images Plaintiff submitted to ProctorU, *id.* ¶ 40; and it was ProctorU that determined how and where to store and use the data generated by Plaintiff's use of ProctorU's service, *see id.* ¶¶ 26-35. Nothing in Plaintiff's Complaint suggests that AWS had any knowledge of those events, or that AWS exercised, or could have exercised, any control over the data involved. Thus, it defies common sense to argue that AWS "possessed" Plaintiff's data. Rather, any such data remained subject to ProctorU's exclusive "dominion and control," and therefore wholly within ProctorU's possession, at all times. *Kuchinski*, 469 F.3d at 861.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Courts have dismissed Section 15(a) claims against other companies acting in a service provider capacity, as AWS allegedly did here, on the same grounds. In *Heard v. Becton, Dickinson & Co.*, for example, the Northern District of Illinois dismissed a Section 15(a) claim against a company that provided fingerprint-based access devices for hospitals. *See* 440 F. Supp. 3d 960, 962 (N.D. Ill. 2020). There, as here, the plaintiff alleged that the defendant "stored" alleged biometric data "in [its] systems." *Id*. at 968. But that was not enough to adequately allege *possession*. Mere storage, the *Heard* court explained, did not suggest "any form of control" or imply that the defendant "could freely access the data." *Id.* at 968-69. The same principle applies here. Plaintiff has alleged, at most, storage and processing by ProctorU on AWS cloud servers. That is not enough to allege possession by AWS under Section 15(a).[5]

Similarly, in *Jacobs v. Hanwha Techwin America, Inc*., a different judge in the Northern District of Illinois dismissed a Section 15(a) claim against a manufacturer and distributor of security cameras that were allegedly used to performed facial recognition on T.J. Maxx shoppers. *See* No. 21 C 866, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021). There, as here, the plaintiff failed to allege that the defendant "exercised control over plaintiff's data or otherwise held plaintiff's data at its disposal." *Id.* at *3 (citation omitted). As a result, the *Jacobs* court could not "draw the reasonable inference that defendant was 'in possession' of [plaintiff's] biometric data." *Id*. Plaintiff's Section 15(a) claim in this case suffers from the same flaw, and it should be dismissed for the same reasons.

In addition to misreading the text of Section 15(a), Plaintiff's attempt to stretch the concept of "possession" to include AWS invites absurd results. *See, e.g.*, *Solon v. Midwest Med. Recs. Ass'n*, 236 Ill. 2d 433, 441 (2010) (when interpreting statutes, courts must "presume that the legislature did not intend absurd, inconvenient, or unjust consequences").

[5] The *Heard* court later allowed the plaintiff's Section 15(a) claim to survive a second motion to dismiss. *See Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 840 (N.D. Ill. 2021). But the court did so only after the plaintiff amended the complaint to add plausible allegations that the defendant "exercise[d] some form of control" over the plaintiff's data. Plaintiff's Complaint includes no such allegations.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Again, where Section 15(a) applies, it requires a private entity to publish a retention and deletion schedule *and* to "permanently destroy[]" biometric data "when the initial purpose for collecting or obtaining" the data "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). But Plaintiff does not explain how AWS could comply with those requirements with respect to data uploaded by customers like ProctorU, nor could she. Plaintiff does not allege that AWS interacts with its customers' end users, including when its customers use Rekognition. Rather, she alleges that "Rekognition is a behind-the-scenes service for businesses" like ProctorU. Compl. ¶ 5. Further, to promote end users' privacy, AWS is contractually prohibited from "access[ing] or us[ing] . . . Content [of customers] except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." Spear Decl., Ex. C ¶ 3.2. As a result, AWS does not know whether (much less when) its customers upload *biometric* data to their S3 buckets. Nor does AWS know whether (much less when) its customers upload biometric data from *Illinois residents*. And if AWS is not even aware of any such data (and certainly not in control of it), then it follows that AWS cannot publish a policy reflecting how and when any such data is deleted.

Similarly, AWS cannot comply with Section 15(a)'s deletion requirements. Again, AWS does not know when its customers, like ProctorU, store *biometric* data from *Illinois* residents. Thus, AWS cannot know when BIPA might apply under Plaintiff's reading of the law. And even if it could, AWS could not determine when BIPA's deletion requirements have been triggered. As a mere back-end service provider, AWS has no way of knowing its customers' "purpose[s]" for collecting end users' data, or when those "purpose[s]" have been "satisfied." 740 ILCS 14/15(a). AWS also has no way of knowing when an end user has "last interact[ed]" with the AWS customer that collected his or her data, because AWS has no relationship with end users. And, of course, if AWS were to delete end users' data contrary to its customers' wishes, then AWS could incur liability to its customers under the parties' contracts and other authorities.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

This case vividly illustrates those threshold problems with Plaintiff's position, which cannot be overstated. ProctorU "provides remote proctoring services for test providers based in at least 45 States," and in 2020 alone, "ProctorU administered approximately 4.6 million tests for more than 1,000 test providers." *Thakkar*, No. 21-CV-2051, Decl. of Dr. Ashley Norris ¶ 7 (Dkt. 21-1). Thus, to comply with Plaintiff's reading of Section 15(a), AWS first would have to determine the residency of millions of ProctorU end users, as well as the types of data that ProctorU collected from those end users. But that is not all. AWS also would have to do that for *all* of the "[m]illions of [other] customers [that] use AWS every day"—not just ProctorU—as well as all of *those* customers' many millions of end users. Compl. ¶ 2. That simply is not possible.

Plaintiff's novel reading of BIPA also would lead to untenable results for large swaths of the economy—not just companies like AWS. For example: Under Plaintiff's reading, companies that provide email services would be deemed to be "in possession" of any and all data attached to their users' email messages or stored in their users' accounts. Thus, to comply with BIPA, those providers would have to scan users' messages for biometric data; identify the people from whom that data was collected, or at least identify their state of residency; and then delete emails subject to BIPA, notwithstanding the wishes of the senders and recipients. That is an impossible burden that BIPA's authors never intended. And equally important, imposing that burden on email providers and other providers would thoroughly undermine the privacy interests of consumers—the very interests Plaintiff purports to champion—by forcing providers to scan, analyze, and even destroy consumers' private data and communications.

For all these reasons, Plaintiff's Section 15(a) claim collapses into incoherence.

2. Plaintiff alleges no facts showing that AWS "collected" her data.

Plaintiff's Section 15(b) claim fails for similar reasons. Section 15(b) applies only to private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. 740 ILCS 14/15(b). (For brevity, AWS uses the word "collect" to encompass all

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

the operative terms.) But Plaintiff does not, and cannot, allege that AWS collected her biometric data within the meaning of Section 15(b).

BIPA does not define Section 15(b)'s operative terms. But the structure of the statute helps reveal their meaning. Because the General Assembly included the term "possession" in Section 15(a) but not in Section 15(b), it follows that mere "possession of biometric data is insufficient to trigger Section 15(b)'s requirements." *Heard*, 440 F. Supp. 3d at 965 (collecting cases). Further, the General Assembly must have meant to distinguish "between possessing and collecting biometric information." *Namuwonge v. Kronos, Inc*., 418 F. Supp. 3d 279, 285-86 (N.D. Ill. 2019). Thus, courts have held that *collection* requires "something more" than mere *possession*. *Jacobs*, 2021 WL 3172967 at *2. And that "something more" is an "affirmative act" or "an active step to collect, capture, purchase, or otherwise obtain biometric data." *Id*.; *see also Heard*, 440 F. Supp. 3d at 966 (same).

Plaintiff does not allege that AWS took any "active step[s]" to collect her data. Indeed, Plaintiff does not even allege that AWS was aware that ProctorU solicited her data. And Plaintiff certainly does not allege that AWS played any role, active or otherwise, in ProctorU's decision to collect data from her. To the contrary, Plaintiff alleges that AWS was nothing more than a passive service provider, while ProctorU determined what data to collect, when to collect it, and what to do with it. *See, e.g.*, Compl. ¶ 34 ("ProctorU requires students to show their faces and their photo IDs on camera to help verify their identities"); *see also, e.g.*, *id*. ¶ 29 (customers like ProctorU "run a command within the Amazon API . . . on the images [they] wish[] to compare"); *id*. ¶ 39 (ProctorU "required [Plaintiff] to submit her image as well as an image of a valid identification document"); *id*. ¶ 40 ("ProctorU used Amazon Rekognition to perform facial recognition on [Plaintiff]"). And once more, it is worth noting that Plaintiff's allegations are entirely consistent with AWS's Customer Agreement, which states that AWS customers like ProctorU "are solely responsible for the development, content, operation, maintenance, and use of [their] Content." Spear Decl., Ex. C ¶ 4.2.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Other courts have dismissed Section 15(b) claims where, here, a plaintiff alleges only that a defendant acted as a third-party technology or service provider, not the active collector of end users' data. *See, e.g.*, *Jacobs*, 2021 WL 3172967 at *3 (dismissing Section 15(b) claim where the defendant was not the "active collector" but rather "merely provided the cameras" that another entity allegedly used to collect biometric data); *Namuwonge*, 418 F. Supp. at 286 (similar; dismissing Section 15(b) claim where the defendant was alleged to have provided technology to another entity and that entity used the technology to collect biometric data); *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *1-2 (Ill. Cir. Ct. Aug. 23, 2019) (similar). This Court should reach the same result.[6]

Here again, Plaintiff's position does not just misread BIPA's language; it also leads to "absurd, inconvenient, [and] unjust consequences" that BIPA's authors never intended. *Solon*, 236 Ill. 2d at 441. Section 15(b) provides that a private entity may not collect biometric data unless it first "(1) informs the subject or the subject's legally authorized representative in writing that [biometric data] is being collected or stored; . . . (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which [biometric data] is being collected, stored, and used; and . . . (3) receives a written release executed by the subject . . . or the subject's legally authorized representative." 740 ILCS 14/15(b). Plaintiff does not explain how AWS and similarly situated cloud-service providers could comply with those detailed notice-and-consent requirements with respect to data they store on behalf of their customers. And for good reason: they simply could not do so. Here, for example, Plaintiff alleges that AWS does not interact directly with ProctorU's end users or any of its customers' end users. *See, e.g.*, Compl. ¶¶ 5, 41, 42. In addition, AWS is contractually prohibited from "access[ing] or us[ing] . . . Content [of AWS customers] except as necessary to

[6] One court has appeared to hold that Section 15(b) may apply to third-party service providers that merely store biometric data. *See Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 779 (N.D. Ill. 2020). AWS respectfully submits that *Figueroa* was wrongly decided, including because the decision fails to explain how passive storage of information, without more, amounts to active collection of data.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." Spear Decl., Ex. C ¶ 3.2. It follows that AWS does not know and cannot know when its customers are collecting *biometric* data, let alone when they are collecting biometric data from *Illinois residents*. How, then, could AWS determine when to provide notice to, and obtain consent from, ProctorU's end users—or any of its customers' end users? Further, given that AWS's customers alone determine why they collect data and how long they retain it, how could AWS inform its customers' end users—*in advance*—of "the specific purpose and length of time" for which their data will be collected? And, putting all that aside, through what mechanism could AWS provide notice to and obtain consent from its customers' end users, given that AWS does not interact with those end users and is a mere "behind-the-scenes service for [other] businesses"? Compl. ¶ 5. Plaintiff does not say. Nor does she acknowledge that the logical implication of her position is that every company that operates via the cloud, including but not limited to email providers, would be subject to BIPA's stringent requirements. And those same companies would, in turn, be forced to adopt extremely intrusive measures to comply with BIPA's requirements—even if they never actively collected biometric data from a single Illinois resident or engaged in any conduct in Illinois.

In *Zellmer v. Facebook, Inc.*, the Northern District of California considered a similarly flawed interpretation of BIPA. There, the plaintiff sought to hold Facebook liable under Section 15(b) for allegedly failing to provide notice to, and obtain consent from, "non-users"—i.e., Illinois residents who merely appeared in photographs uploaded to Facebook by Facebook users, but who did not themselves have any relationship with Facebook. The *Zellmer* court rejected the claim, reasoning that it would be "patently unreasonable to construe BIPA to mean that" companies are "required to provide notice to, and obtain consent from," end users "who [are] for all practical purposes total strangers" to the companies. No. 3:18-cv-01880-JD, 2022 WL 976981, at *3 (N.D. Cal. Mar. 31, 2022). Instead, the court reasoned, the "Illinois legislature clearly contemplated that BIPA would apply [only] in situations where a business had at least

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

some measure of knowing contact with and awareness of the people subject to biometric data collection." *Id*. at *4. Any other interpretation "would lead to obvious and insoluble problems," *id*.; "put [companies] in an impossible situation"; and "impose extraordinary burdens on businesses," contrary to "the Illinois legislature's intent," *id*. at *5.

The same reasoning applies here. According to Plaintiff, AWS has "[m]illions of customers," "[t]housands" of whom use Rekognition. Compl. ¶¶ 2, 4. It is simply not possible for AWS to identify, notify, and obtain consent from millions of end users of AWS customers. Even if it was possible in theory, it would impose mind-boggling burdens on AWS in practice, contrary to the General Assembly's intent. *See Zellmer*, 2022 WL 976981, at *5 (according to the Illinois Supreme Court, "BIPA should not impose extraordinary burdens on businesses"). Fortunately, nothing in BIPA purports to impose such impossible demands. Section 15(b) applies only "where a business ha[s] at least some measure of knowing contact with and awareness of the people subject to biometric data collection." *Id*. at *4. This is not one of those cases.

B. Plaintiff's Claims Should Be Dismissed Under the Illinois Extraterritoriality Doctrine and the U.S. Constitution's Dormant Commerce Clause

All of Plaintiff's claims fail for the further reason that Plaintiff has not alleged, and could not allege, that AWS's purported misconduct occurred primarily and substantially in Illinois.

1. Plaintiff's claims violate the extraterritoriality doctrine.

"BIPA does not contain an express provision stating it is intended to apply extraterritorially," i.e., beyond the borders of Illinois. *McGoveran v. Amazon Web Servs., Inc.*, No. 20-cv-1399-LPS, 2021 WL 4502089, at *3 (D. Del. Sept. 30, 2021). Thus, BIPA applies only if the defendant's alleged conduct "occurred primarily and substantially in Illinois." *Avery*, 216 Ill. 2d 100 at 187.

Here, Plaintiff does not plead facts showing that AWS engaged in *any* conduct in Illinois, let alone that AWS's relevant conduct occurred "primarily and substantially" in Illinois. *Id*. Instead, Plaintiff merely alleges that (1) she attended the Colleges in Illinois; (2) the Colleges

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

"requir[ed]" her to use "ProctorU's software"; (3) she disclosed images of herself to ProctorU via ProctorU's service; and (4) ProctorU then "used Amazon Rekognition to perform facial recognition" on those images. Compl. ¶¶ 37-40. But neither AWS nor ProctorU are Illinois-based companies. *See id*. ¶ 9 (AWS is "a Delaware corporation with its headquarters in Seattle, Washington"); *see also* Spear Decl., Ex. E (Alabama Secretary of State record indicating that ProctorU is a Delaware corporation with its headquarters in Birmingham, Alabama).[7] Further, Plaintiff does not allege that ProctorU's S3 bucket is located in Illinois; that ProctorU used Rekognition in Illinois; or that Plaintiff interacted with AWS in Illinois. *See id.* ¶¶ 41, 42. Thus, her allegations do not suggest that AWS engaged in *any* Illinois conduct whatsoever.

This case is much like *McGoveran*, where the District of Delaware dismissed strikingly similar BIPA claims against AWS under the extraterritoriality doctrine. In *McGoveran*, the plaintiffs were Illinois residents who contacted the telephone call centers of John Hancock, a financial services company. *See McGoveran*, 2021 WL 4502089, at *2. Plaintiffs alleged that, when they called John Hancock, their voices were recorded and analyzed by Pindrop Security, a Georgia company acting on John Hancock's behalf. *See id*. Plaintiffs further alleged that Pindrop analyzed those recordings to generate "voiceprints," which plaintiffs characterized as biometric data governed by BIPA. *Id*. And, according to plaintiffs, Pindrop then stored the voiceprints on AWS's servers. *See id*. Based on those allegations, plaintiffs sued AWS and Pindrop under BIPA. AWS moved to dismiss plaintiffs' claims, arguing that the "complaint allege[d] an improperly extraterritorial application of BIPA." *Id*. at *1. The court agreed and dismissed plaintiffs' claims, reasoning as follows:

- First, the court noted that plaintiffs did not allege that their "voiceprints" were "created, possessed, or stored . . . in Illinois." *Id*. at *4.

[7] The Court may take judicial notice of the fact that ProctorU is incorporated in Delaware and based in Alabama because "courts routinely take judicial notice of a company's certificate of incorporation on a motion to dismiss." *In re Coinstar Inc. S'holder Derivative Litig.*, No. C11-133 MJP, 2011 WL 5553778, at *2 (W.D. Wash. Nov. 14, 2011) (citations omitted).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

- Second, "AWS emphasize[d] that its data centers [were] located wholly outside Illinois . . . and Plaintiffs [did] not allege otherwise." *Id*.

- Third, the court rejected the argument that AWS's purported failure to provide BIPA-compliant notice and obtain BIPA-compliant consent occurred in Illinois, both because it "really makes no sense to assign a location for an act that did not occur," and because, "[m]ore fundamentally, that argument depends on the assumption that [AWS was] required to" comply with BIPA in Illinois, but plaintiffs did not allege "any activity in Illinois that would impose such obligations on [AWS]." *Id*.

- Fourth, "[a]t bottom," the only alleged connection between the case and Illinois was plaintiffs' residency in Illinois. But a "plaintiff's residency is not enough to establish an Illinois connection in order to survive a motion to dismiss based on extraterritoriality." *Id*. (citing cases).

In sum, based on plaintiffs' allegations, the *McGoveran* court concluded that "John Hancock's activities . . . might be ascribed to Illinois." *Id.* at *6. But "the same [could not] be said for Pindrop and AWS, who were merely third-party contractors performing work for John Hancock." *Id*. The Court therefore dismissed plaintiffs' claims against AWS under the extraterritoriality doctrine. *See id*.[8]

Here, as in *McGoveran*, Plaintiff seeks to hold AWS liable in its capacity as a back-end service provider to another company (ProctorU), even though AWS has no direct relationship with Plaintiff and even though AWS has never interacted with Plaintiff in Illinois or elsewhere. Moreover, as in *McGoveran*, Plaintiff does not, and cannot, allege that the biometric data supposedly at issue—i.e., alleged scans of Plaintiff's face geometry—were "created, possessed, or stored . . . in Illinois." *Id*. at *4. And finally, as in *McGoveran*, Plaintiff relies entirely on the mere fact of her Illinois residency to argue that AWS should be held liable under BIPA. *See, e.g.*, Compl. ¶¶ 8, 37-43. But as the *McGoveran* court made clear, "[a] plaintiff's residency is not enough to establish an Illinois connection in order to survive a motion to dismiss based on extraterritoriality." *McGoveran*, 2021 WL 4502089, at *4.

[8] Later, the *McGoveran* court allowed plaintiffs' claims to proceed after they amended their complaint to add specific allegations suggesting that AWS's conduct "occurred principally and substantially" in Illinois. *Id*. (Dkt. 46). Plaintiff's Complaint includes no such allegations.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

2. Adopting Plaintiff's sweeping interpretation of BIPA would violate the U.S. Constitution's Dormant Commerce Clause.

The U.S. Constitution's Dormant Commerce Clause "protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 335-37 (1989). For example, in *Sam Francis Foundation v. Christies, Inc.*, the Ninth Circuit struck down a California law that "require[d] the payment of royalties to the artist after a sale of fine art whenever 'the seller resides in California or the sale takes place in California.'" 784 F.3d 1320, 1323 (9th Cir. 2015) (citation omitted). The Ninth Circuit held that requirement amounted to an "impermissible regulation of wholly out-of-state conduct" because it regulated "out-of-state art sales" with "no other connection" to the state beyond the seller's residency. *Id.* at 1324 (citation omitted).

Here, Plaintiff asks the Court to interpret BIPA so that it sweeps just as broadly as the law invalidated in *Sam Francis Foundation*. More specifically, Plaintiff asks this Court to impose BIPA's requirements on AWS's out-of-state conduct simply because Plaintiff happens to reside in Illinois. But the Dormant Commerce Clause does not allow states to project their authority that broadly; rather, it "precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the state." *Healy*, 491 U.S. at 336. And this case shows the wisdom of that rule. As the *McGoveran* court observed, it would be both "overly broad and ultimately untenable" to hold that BIPA applies whenever a plaintiff resides in Illinois. *McGoveran*, 2021 WL 4502089, at *6. After all, "if that rule were correct, then BIPA could impose liability on a vast number of corporations who do no business in Illinois and who lack any other significant connection to Illinois." *Id*. The Dormant Commerce Clause forbids that result.

C. BIPA's Financial Institutions Exemption Bars Plaintiff's Claims

Putting aside the other fatal flaws described above, Plaintiff's claims should be dismissed because they violate the plain language of Section 25(c) of BIPA.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

1. BIPA may not be applied to "financial institutions," which includes colleges and universities that administer financial aid.

Financial institutions "are already subject to a comprehensive privacy protection regime under" the federal Gramm-Leach-Bliley Act ("GLBA") and its regulations. *Bryant v. Compass Grp. USA, Inc*., 503 F. Supp. 3d 597, 601 (N.D. Ill. 2020). Accordingly, to avoid subjecting those institutions to redundant and contradictory requirements, BIPA's authors exempted them from BIPA's scope entirely. In particular, Section 25(c) of BIPA provides that the law does not apply "in any manner to a financial institution or an affiliate of a financial institution that is subject to [the GLBA] and the rules promulgated thereunder." 740 ILCS 14/25(c).

"Financial institution" is a term of art defined by the GLBA and its regulatory scheme. Crucially for this case, the term includes educational institutions that administer financial aid. *See, e.g.*, Fed. Trade Comm'n, Privacy of Consumer Financial Information, 65 Fed. Reg. 33648 (May 24, 2000) (explaining that "institutions of higher education" are financial institutions because "[m]any, if not all, such institutions appear to be significantly engaged in lending funds to consumers"). Courts have therefore held that Section 25(c) prohibits applying BIPA to the activities of colleges and universities, *including in the remote proctoring context*. For example, in *Doe v. Northwestern University*, the plaintiff alleged that she was a student at Northwestern University; that Northwestern required her to use "third-party online remote proctoring tools"; and that those third-party services collected and stored her biometric data in violation of BIPA. No. 21 C 1579, 2022 WL 1485905, at *1 (N.D. Ill. Feb. 22, 2022). The court dismissed plaintiff's claims, holding that Northwestern was a financial institution and therefore "exempt from BIPA." *Id*. at *3. Even more recently, a different court dismissed similar BIPA claims against Bradley University for the same reasons. *See Duerr v. Bradley Univ*., No. 1:21-CV-01096-SLD-JEH, 2022 WL 1487747, at *7 (C.D. Ill. Mar. 10, 2022).

2. Allowing Plaintiff's claims to proceed would impermissibly apply BIPA's requirements to the Colleges, which are financial institutions.

Here, BIPA's financial institutions exemption requires dismissal of Plaintiff's claims.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

First, just like Northwestern University and Bradley University, Plaintiff's Colleges are financial institutions. Like many other institutions of higher learning, the Colleges administer financial aid for their students, and they have been identified by the Federal Student Aid office of the U.S. Department of Education as participants in the Title IV federal student aid program. *See* Spear Decl., Ex. F at 11 (listing schools that participate in the Title IV federal student aid program, including the Colleges); *see also Northwestern Univ.*, 2022 WL 1485905 at *2 (relying on "publicly available government documents" to establish that university offered financial aid). Thus, the Colleges are exempt from BIPA's requirements under Section 25(c).

Second, the practical effect of applying BIPA to AWS in this context would be to apply BIPA to the Colleges, which is precisely what Section 25(c) forbids.

Plaintiff acknowledges, as she must, that the remote proctoring activities giving rise to her claims are *the Colleges'* activities. *See* Compl. ¶ 38 (alleging that the Colleges "requir[ed]" Plaintiff to use "ProctorU's software"). It follows that Section 25(c) prohibits applying BIPA to those activities. *See Northwestern Univ.*, 2022 WL 1485905 at *3 (dismissing BIPA claims against university based on university's remote proctoring program); *Duerr*, 2022 WL 1487747 at *7 (same). Plaintiff, however, contends that AWS must provide BIPA-compliant notices to the Colleges' students whenever they use ProctorU's software. *See* Compl. ¶¶ 68, 69. She also contends that AWS must obtain BIPA-compliant "written releases" from the Colleges' students. *Id*. ¶ 67. And, it appears, Plaintiff also believes that AWS must delete students' data according to BIPA's requirements, notwithstanding the wishes of ProctorU and the Colleges. Of course, forcing AWS to inject itself into the Colleges' remote proctoring activities in those ways would necessarily interfere with the Colleges' activities, including by forcing the Colleges and ProctorU to redesign the interfaces through which "students sign in to ProctorU to take a test." *Id*. ¶ 35. Indeed, practically speaking, Plaintiff's BIPA claims would subject the Colleges' remote proctoring activities to all of BIPA's requirements, just from the "bottom up" rather than from the "top down." Section 25(c) does not allow that result.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

In response, Plaintiff may argue that she is not seeking to hold the Colleges liable under BIPA. She may also argue that requiring the Colleges to modify their remote proctoring programs to accommodate her reading of BIPA would impose a minor burden on the Colleges. But Section 25(c) prohibits applying BIPA to the Colleges "in *any* manner." 740 ILCS 14/25(c) (emphasis added). Thus, it requires the Court to reject any reading of BIPA that would impose BIPA's requirements on the Colleges' activities—even indirectly or to a limited extent. *Cf. Stevenson v. FedEx Ground Package Sys., Inc.*, 69 F. Supp. 3d 792, 796 (N.D. Ill. 2014) (Illinois law prohibited interfering with employees' rights "in any manner whatsoever"; court interpreted that language to prohibit even "minor" and "de minimis" interference). Any other reading would require the Court to ignore Section 25(c)'s "in any manner" language, violating basic canons of statutory construction. *See Chestnut Corp. v. Pestine, Brinati, Gamer, Ltd.*, 667 N.E.2d 543, 547 (Ill. App. Ct. 1996) ("Statutes are to be construed to give full effect to each word, clause, and sentence, so that no word, clause, or sentence is surplusage or void.") (citation omitted).

D. Plaintiff Cannot Be "Aggrieved" by AWS's Alleged Violation of Section 15(a)

Plaintiff's Section 15(a) claim fails for an additional and independent reason: Plaintiff cannot show that she is "aggrieved" by AWS's alleged violation of Section 15(a), which is a threshold requirement for bringing a claim under BIPA.

Only an "aggrieved" person may seek relief under BIPA. 740 ILCS 14/20. And to be aggrieved, a plaintiff must "hav[e] legal rights that are adversely affected" or "invaded" by the defendant's conduct. *Rosenbach*, 129 N.E.3d at 1205. Thus, to show that she is aggrieved for purposes of her Section 15(a) claim, Plaintiff must plausibly allege both that (1) AWS violated a legal duty under Section 15(a), and (2) that AWS owed that legal duty to Plaintiff. *See, e.g.*, *Am. Sur. Co. v. Jones*, 51 N.E.2d 122, 125 (Ill. 1943) (appellants were not "aggrieved" because the action of which they complained "did not directly affect [their] interest"); *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 546 (N.D. Cal. 2018) (holding that "a party is aggrieved" under BIPA "by an act that directly or immediately affects her legal interest").

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Plaintiff cannot meet those requirements. She alleges that AWS violated Section 15(a) by "fail[ing] to publicly provide a retention schedule or guideline for permanently destroying" biometric data. Compl. ¶ 58. But "the duty to disclose under section 15(a) is owed to the public generally, *not to particular persons*." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020) (emphasis added). Plaintiff has therefore alleged, at most, that AWS violated a duty owed to *the public*, not to *her*. Thus, she is not "aggrieved," and her claim necessarily fails.

* * *

MOTION TO STRIKE CLASS ALLEGATIONS UNDER RULE 12(f)

Under Rule 12(f), the Court "may order stricken from any pleading any insufficient defense or any redundant, immaterial, impertinent, or scandalous matter." Striking class allegations is appropriate "[w]here the face of the complaint demonstrates that a class action cannot be maintained on the alleged facts." *Abdelfattah v. Carrington Mortg. Servs. LLC*, No. C-12-04656-RMW, 2013 WL 5718463, at *1 (N.D. Cal. Oct. 21, 2013) (citation omitted).

Here, Plaintiff's proposed class is wildly improper on its face. Plaintiff does not seek to represent a class of people who, like her, used ProctorU's identity-verification services. Instead, she seeks to represent every Illinois resident who has ever had his or her biometric data "obtained by Amazon's Rekognition service and stored in AWS's servers." Compl. ¶ 44. In other words, Plaintiff seeks to represent *every* Illinoisian who has interacted with *every* one of the "[t]housands" of companies that incorporate Rekognition into their products and services—not just ProctorU. *Id.* ¶ 4. As a result, Plaintiff cannot meet two basic requirements for certification of a Rule 23(b)(3) class: she cannot show that her claims are "typical" of class members' claims, and she cannot show that common issues would predominate over individual issues.[9]

[9] Plaintiff may also be seeking certification under Rule 23(b)(2). That would be inappropriate for at least two reasons. First, Rule 23(b)(2) certification is not available where, as here, the plaintiff primarily seeks monetary relief. *See Linehan v. AllianceOne Receivables Mgmt., Inc.*, No. C15-1012-JCC, 2016 WL 9526500, at *4 (W.D. Wash. Nov. 22, 2016). Second, Rule 23(b)(2) certification is inappropriate where the plaintiff seeks injunctive relief that amounts to nothing more than "a bare injunction to follow the law," *Parsons v. Ryan*, 754 F.3d 657, 689 n.35 (9th Cir. 2014), which is all that Plaintiff seeks here, *see* Compl. at 17.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

First, Plaintiff could not possibly establish typicality. According to Plaintiff, she interacted with only one Rekognition-using AWS customer: ProctorU. She did not interact with any other AWS customers that use Rekognition, of which there are "[t]housands." Thus, as a logical matter, Plaintiff's claims cannot be typical of the class's claims, because her class—as alleged—includes vast number of people who share none of her experiences. *See Miller v. Dollar Tree Stores, Inc.*, No. CV-06-019-RHW, 2006 WL 8438078, at *6 (E.D. Wash. Oct. 13, 2006) (striking class allegations where plaintiff, who worked just six days during store's pre-opening, was not typical of the class of employees she sought to represent).[10]

Second, Plaintiff cannot show that common issues would predominate. *See, e.g.*, *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011) (the mere fact that members of a proposed class "have all suffered a violation of the same provision of law" does not justify class treatment; rather, there must be a "common contention" that is "central to the validity of each one of the claims" and that will be resolved "in one stroke"). Among other things, BIPA's notice and consent elements would require individualized proof for each of the "[t]housands" of AWS customers that use Rekognition "for a wide variety of use cases," including "user verification," "cataloging," and "people counting." *Id*. at ¶¶ 4, 23. Presumably, each of those "[t]housands" of companies used their own unique forms of notice and consent and adopted their own unique deletion policies. (Plaintiff does not allege otherwise.) Further, given that many of these use cases do not involve facial analysis at all, *see* Spear Decl., Ex. G (describing Rekognition's text detection, object labeling, logo detection, package detection, and other capabilities), individualized proof would also be necessary to determine (1) whether each of those thousands of AWS customers used Rekognition in a manner that generated "biometric identifiers" or "biometric information" within the meaning of BIPA, *see* 740 ILCS 14/10, and (2) if so, whether

[10] For the sake of comparison, the plaintiffs in the *Thakkar v. ProctorU, Inc.* case seek to represent a class of "all Illinois residents who used ProctorU to take an exam online and who had their facial geometry collected, captured, received, or otherwise obtained and/or stored by" ProctorU. No. 21-CV-2051, Am. Compl. ¶ 68 (Dkt. 18).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

AWS controlled any such data given how each AWS customer structured its software systems and used AWS's services. *See, e.g.*, *Poshville, Inc. v. Pawnee Leasing*, No. 2:21-CV-01465-SVW-AGR, 2021 WL 4776708, at *1 (C.D. Cal. July 15, 2021) (striking class allegations even though the defendants "may use somewhat similar business methods in dealing with different clients" because "each client ultimately has unique negotiations, contracts, equipment, and damages that are not suitable for a class action"). It follows that Plaintiff's class suffers from so much inherent complexity that individualized issues necessarily would predominate. Certification is therefore improper. *See, e.g.*, *Amchem Prod., Inc. v. Windsor*, 521 U.S. 591, 624 (1997) (certification improper because "[c]lass members were exposed to different asbestos-containing products, for different amounts of time, in different ways, over different periods") (citations and quotation marks omitted); *Lapekas v. Kaiser Found. Health Plan, Inc.*, No. 10-cv-5984-VBF-FMOx, 2011 WL 13217477, at *3 (C.D. Cal. May 25, 2011) (denying certification where defendant "offer[ed] many different health care plans" and the plaintiff could not show "sufficient common issues of law or fact across all health plans"); *see also Cashatt v. Ford Motor Co.*, No. 3:19-CV-05886-RBL, 2020 WL 1987077, at *6 (W.D. Wash. Apr. 27, 2020) (striking class allegations because individualized issues would "far outstrip" common ones).

CONCLUSION

AWS respectfully requests that the Court dismiss Plaintiff's claims under Rule 12(b)(6), with prejudice, and strike Plaintiff's class allegations under Rule 12(f).

Dated: May 16, 2022

By: */s/ Ryan Spear*

Ryan Spear, WSBA No. 39974
RSpear@perkinscoie.com
Nicola Menaldo, WSBA No. 44459
NMenaldo@perkinscoie.com
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone 206.359.8000
Facsimile 206.359.9000

Attorneys for Defendant
AMAZON WEB SERVICES, INC.